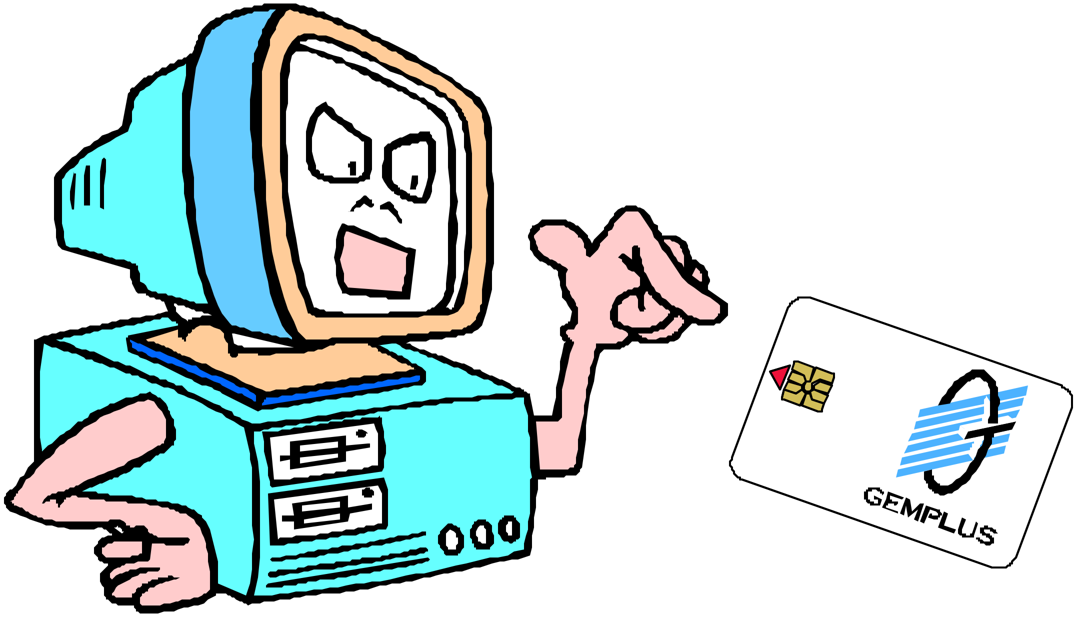
Introduction to Smart Card Technology



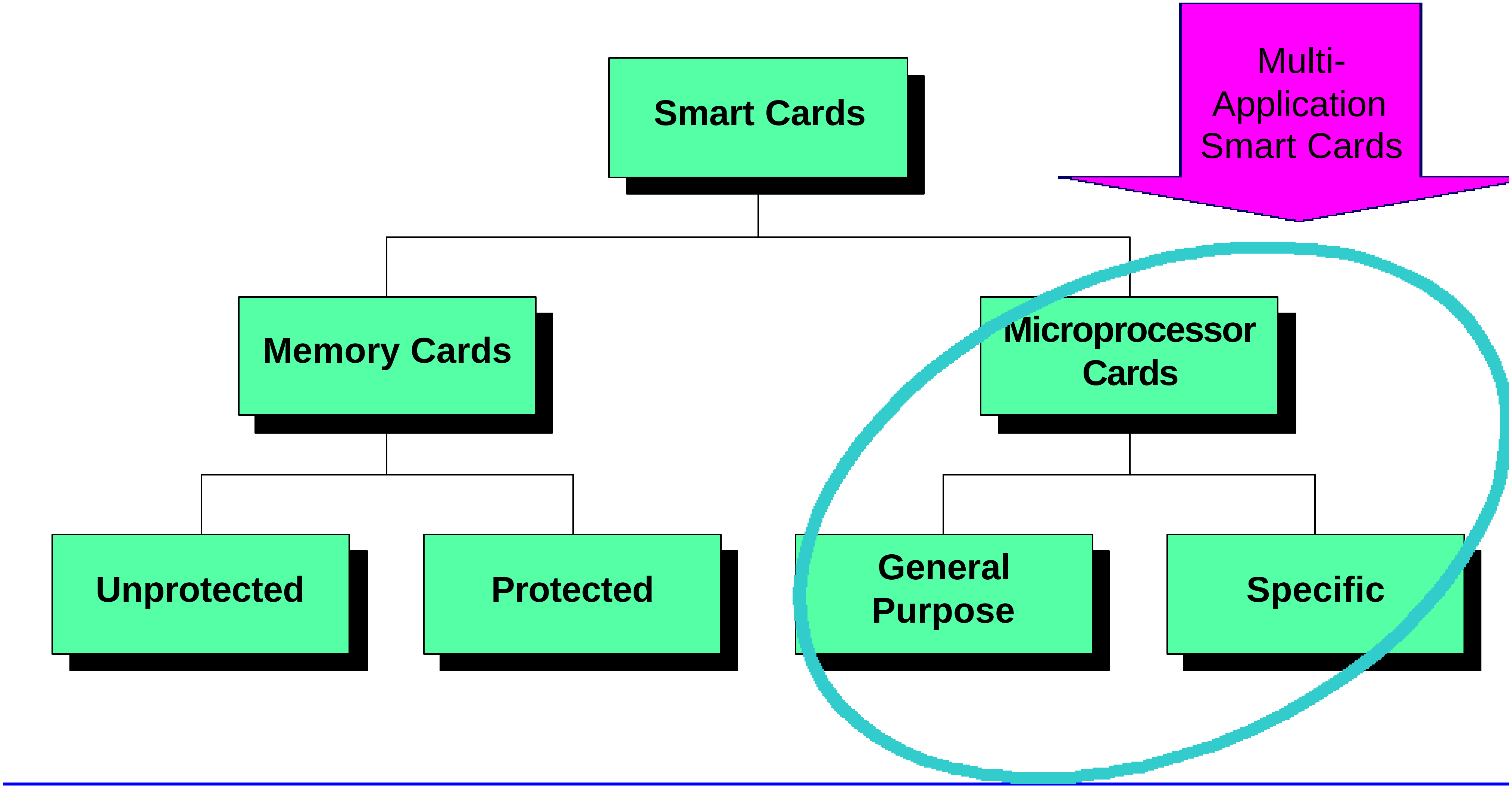
Gilles Lisimaque

Chief Technology Officer

Gemplus Corp.

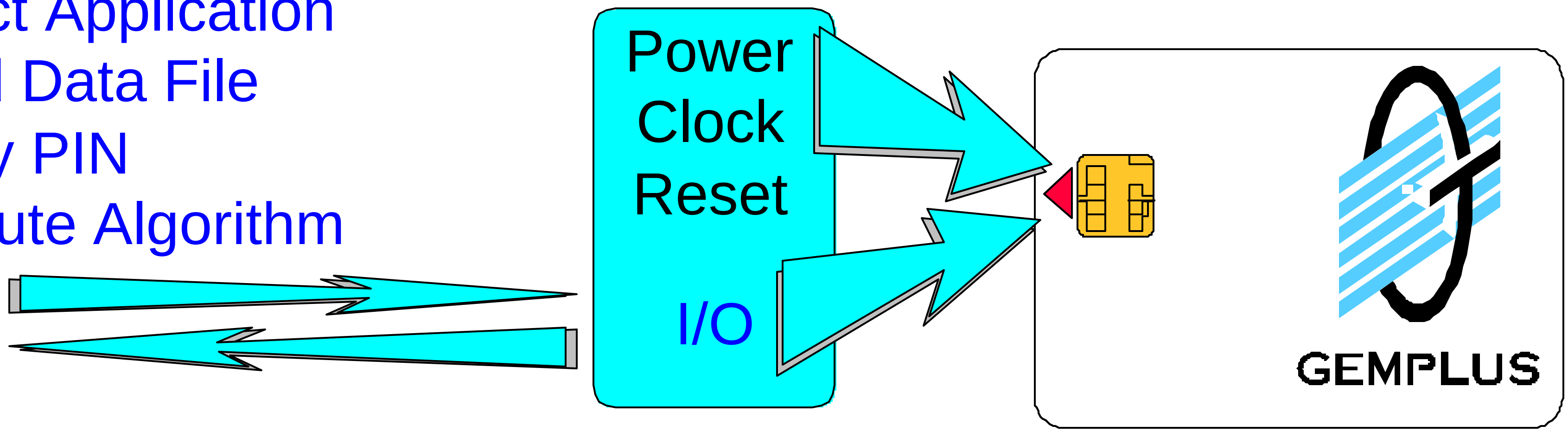
GEMPLUS

A Wide Range of Capabilities



A Smart Card is a Small Computer

Commands:
- Select Application
- Read Data File
- Verify PIN
- Execute Algorithm
- ....



Power
Clock
Reset

I/O

Application

Standard Interface

Smart Card

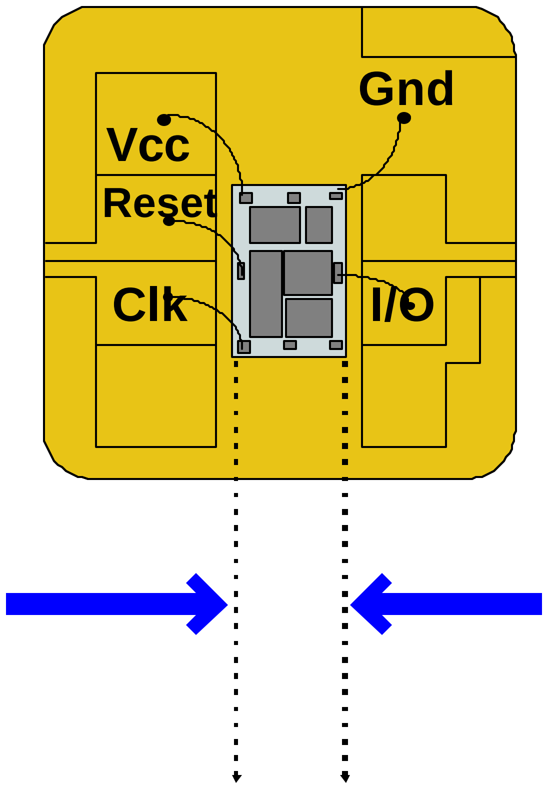
Microprocessor smart cards are intelligent active devices with adapting behavior and active defenses

Mechanical Constraints

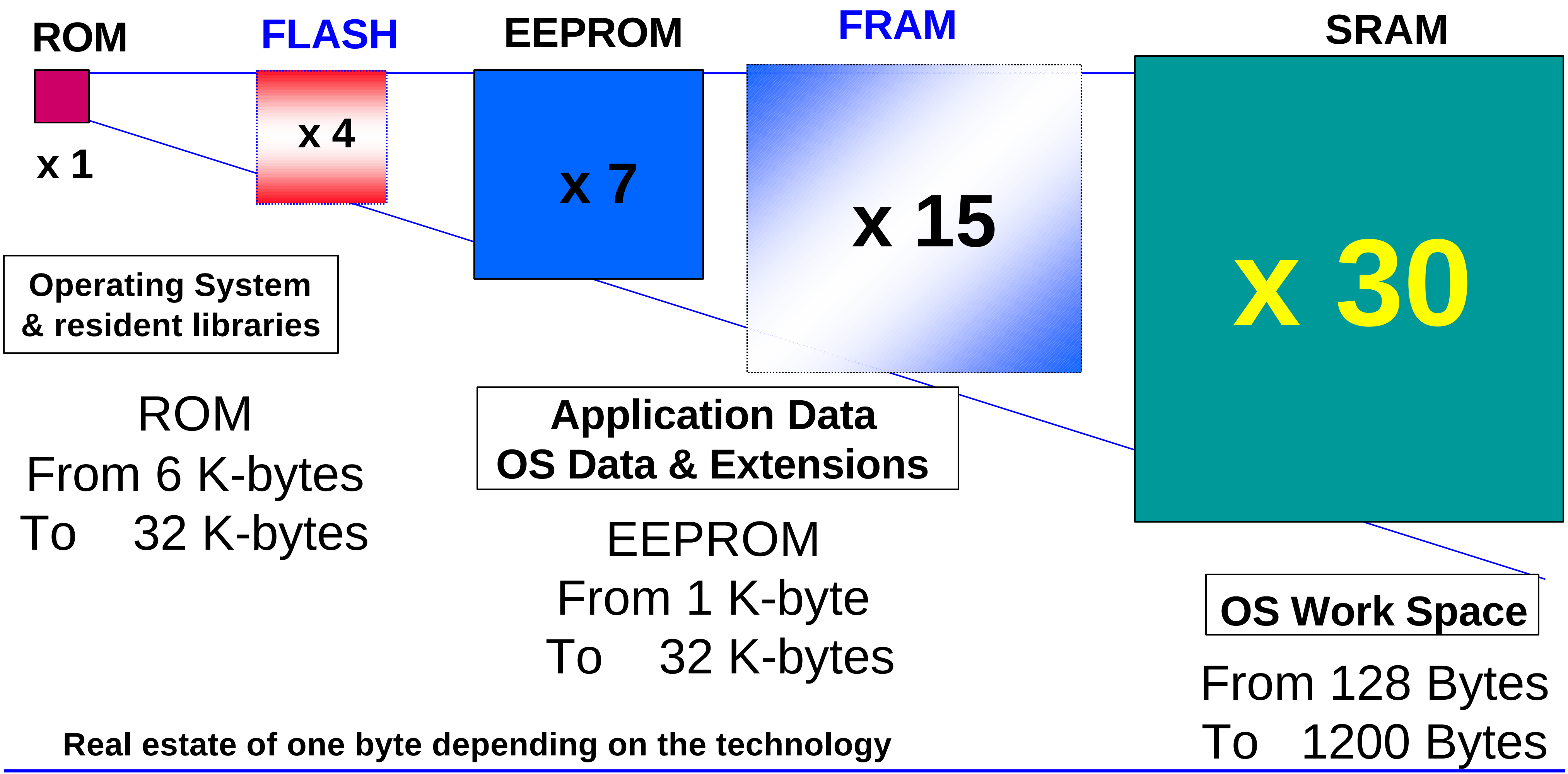
- ISO defines amplitude of flexion/torsion for plastic cards.

  As a practical result:

  - the die size should be less than 25 mm^2 (38,000 square mils)
  - The greater die dimension should be on the shorter card axis



Smart Card Silicon Real Estate



Operating System
& resident libraries

ROM
From 6 K-bytes
To 32 K-bytes

Application Data
OS Data & Extensions

EEPROM
From 1 K-byte
To 32 K-bytes

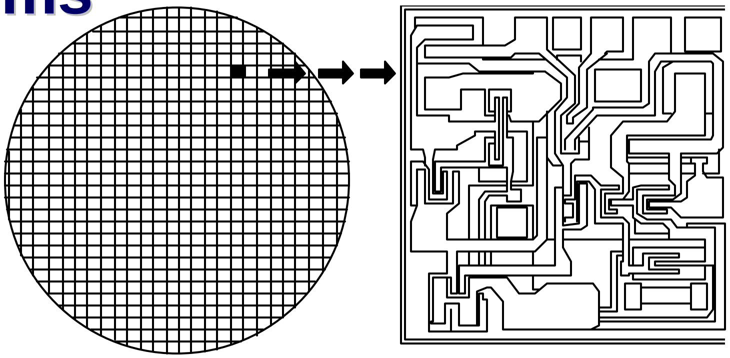
OS Work Space

From 128 Bytes
To 1200 Bytes

Real estate of one byte depending on the technology

Smart Card Silicon CPU Power

- 8 bit microprocessor used in most smart cards
  - 6805 / 8051 / H8
- Specialized crypto coprocessor for recent chips designed to run public key algorithms

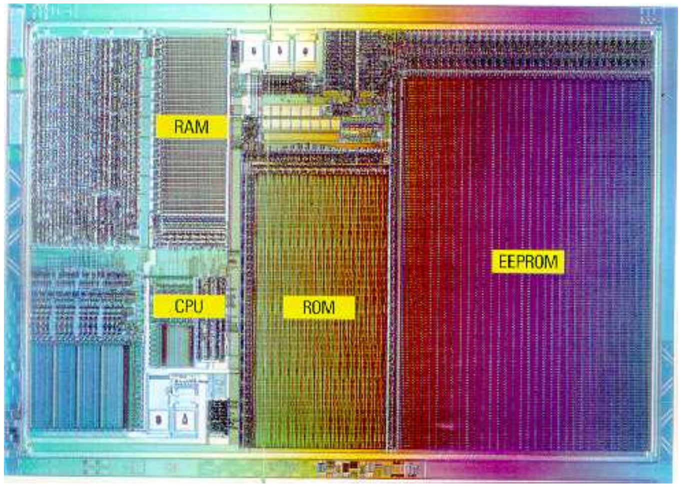


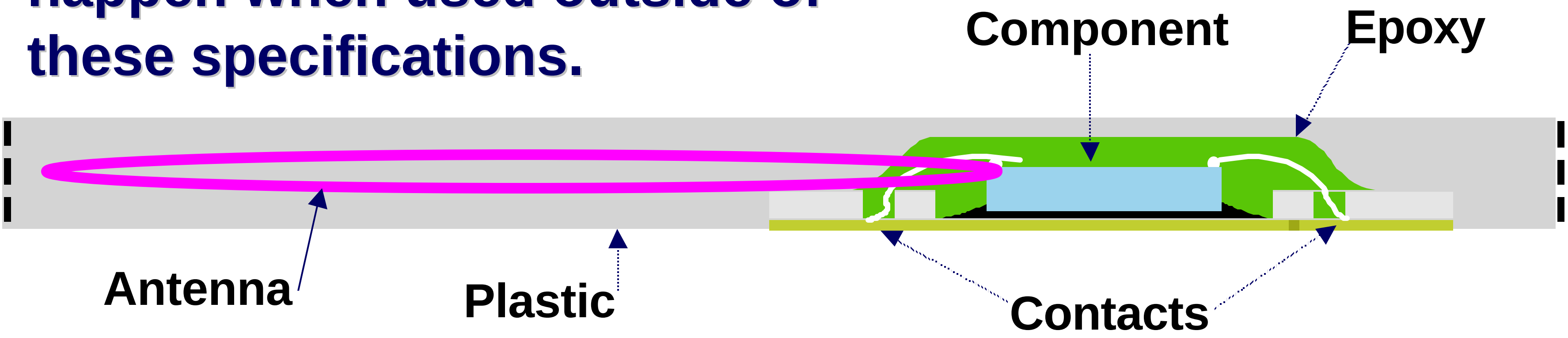
- 32-bit RISC Available
  - Biometrics
  - Advanced Cryptography
  - Applications applets and objects management (in some JavaCard^{TM} implementations)
- Internal clock goes up to 20Mhz in some chips

Behind the Contacts
A Secure Component

A Smart Card component monitors its environment to detect hackers.

Not only must it work within its specifications, but it must not allow a security breach to happen when used outside of these specifications.




Component

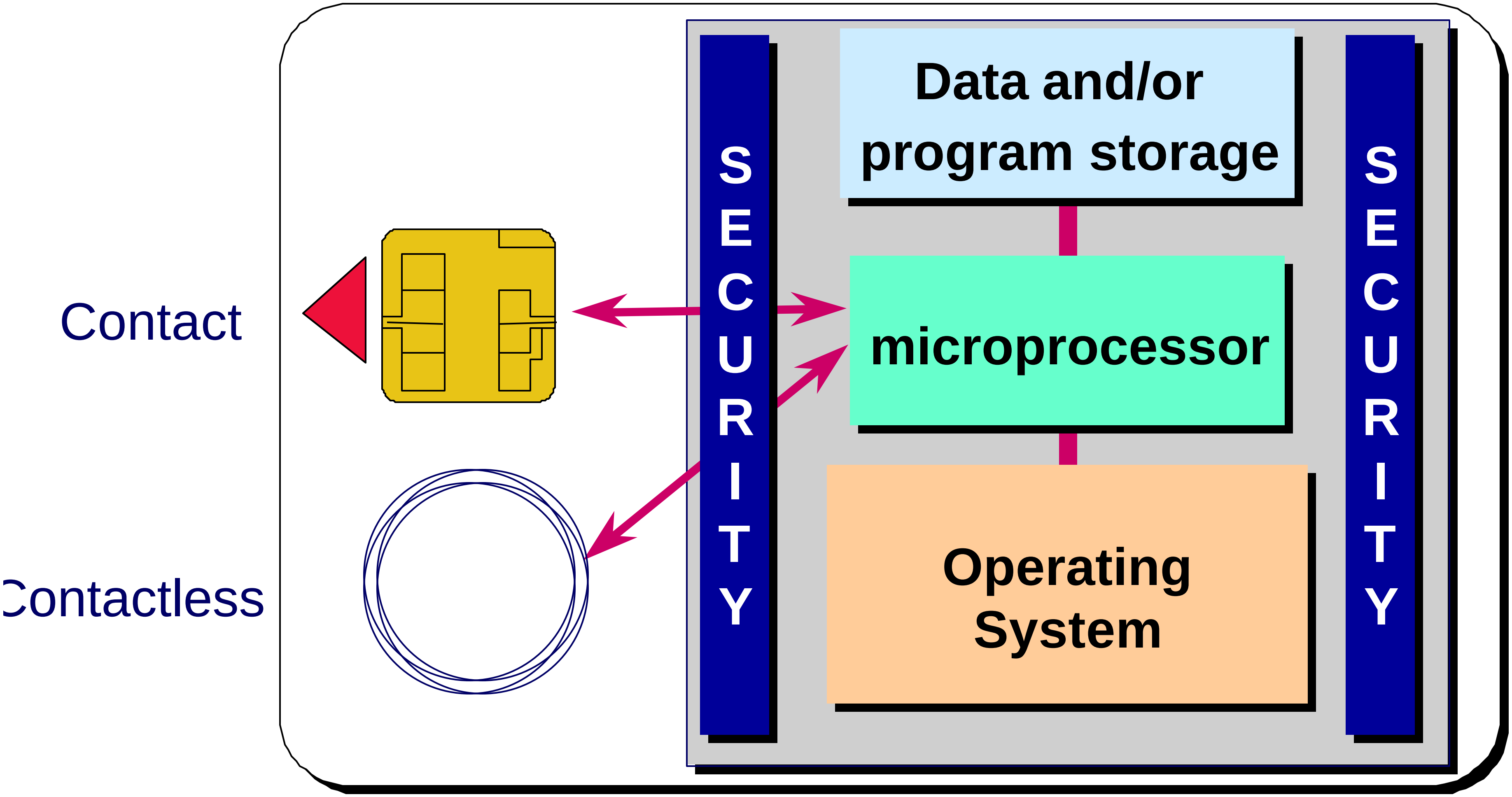
Epoxy

Antenna

Plastic

Contacts

Smart Card Resources



Contact

Contactless

SECURITY

Data and/or program storage

microprocessor

Operating System

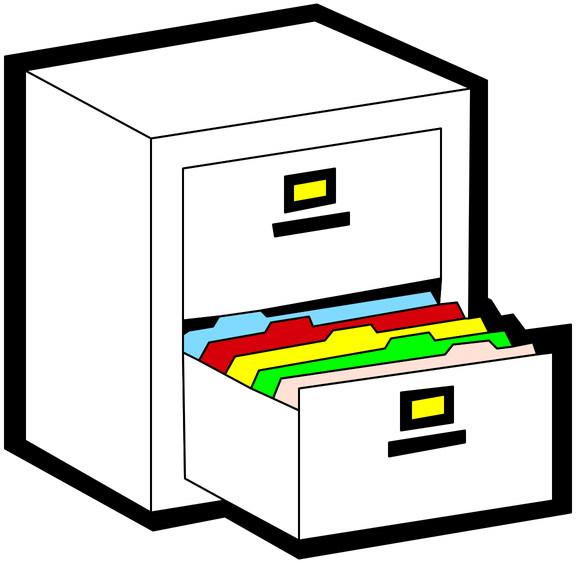
SECURITY

The resources managed by the OS are the serial I/Os, the memory and the security

The Functions of a Smart Card OS

- I/O Management
  - interrupts, I/O exchanges, transport protocol
- Data Management
  - memory, file, directories, tags, objects
  - data integrity (e.g. commit, rollback)
- Security Related Functions
  - algorithms, key generation, key management
- Application Generic Functions
  - cardholder verification method (password)
  - electronic purse management

Data Management



- **Directory and File Structure**
  - **Transparent files**
  - **Record management**
    - Fixed or variable length
    - Linear or cyclic files
- **Object Management (Object Tags)**
- **Relational Data Base**

Smart Card Life Cycle

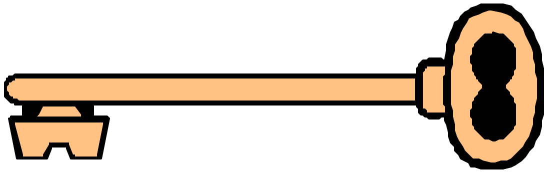
- **Manufacturing**
  - **During the manufacturing of the chip a unique manufacturing serial number is written in the chip**

- **Initialization**
  - **Permanent applications are loaded in the chip**
- **Personalization**
  - **Information related to the specific cardholder is loaded**
- **Application(s)**
  - **Applications can update their information, new applications can be downloaded, old may be removed**
- **End-of-life**
  - **Because the plastic ages quite quickly, the card technology and the security is improved permanently, smart cards are often replaced every two or three years**

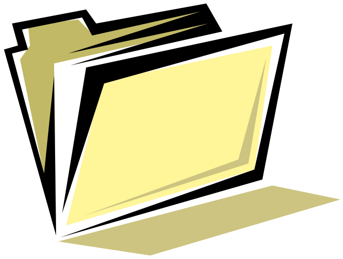
Managed by the Card Operating System, from cradle to grave

Why use a smart card ?

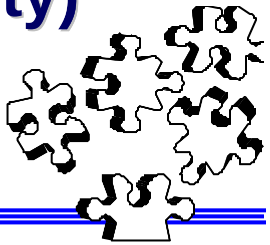
- As a unique physical identifier (provides identification)
  - Smart Cards have a unique serial number.
    - Physical access control
    - Security token entry index in a database



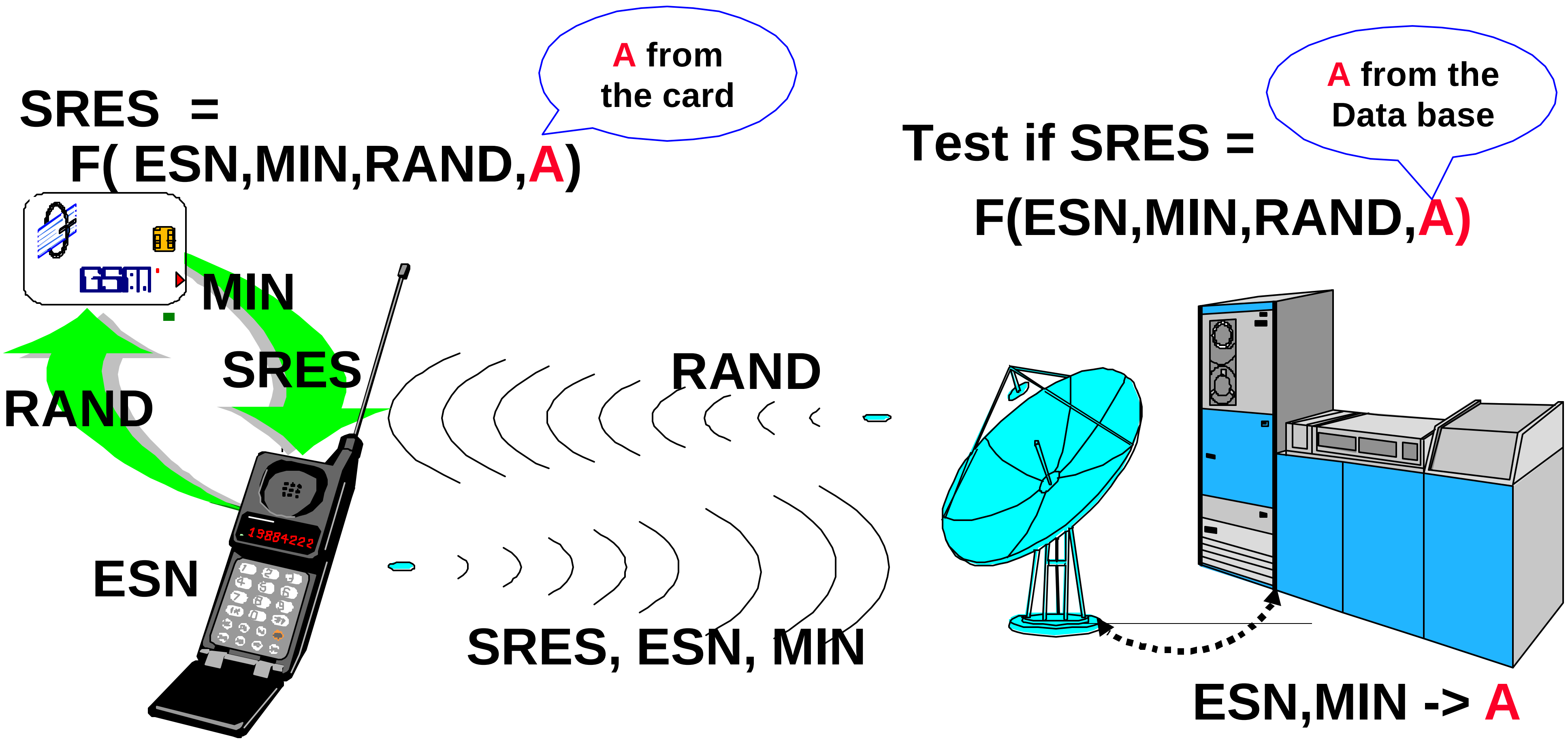
- As a secure Data Carrier (provides mobility)
  - Smart Cards can protect access to files stored in their memory
    - Identification token, data carrier
    - Medical Insurance



- As an application secure processor (provides security)
  - “sensitive” process is done in the smart card



PCS Subscriber Identification



SRES =
F(ESN,MIN,RAND,A)

A from the card

Test if SRES =
F(ESN,MIN,RAND,A)

A from the Data base

MIN

SRES

RAND

RAND

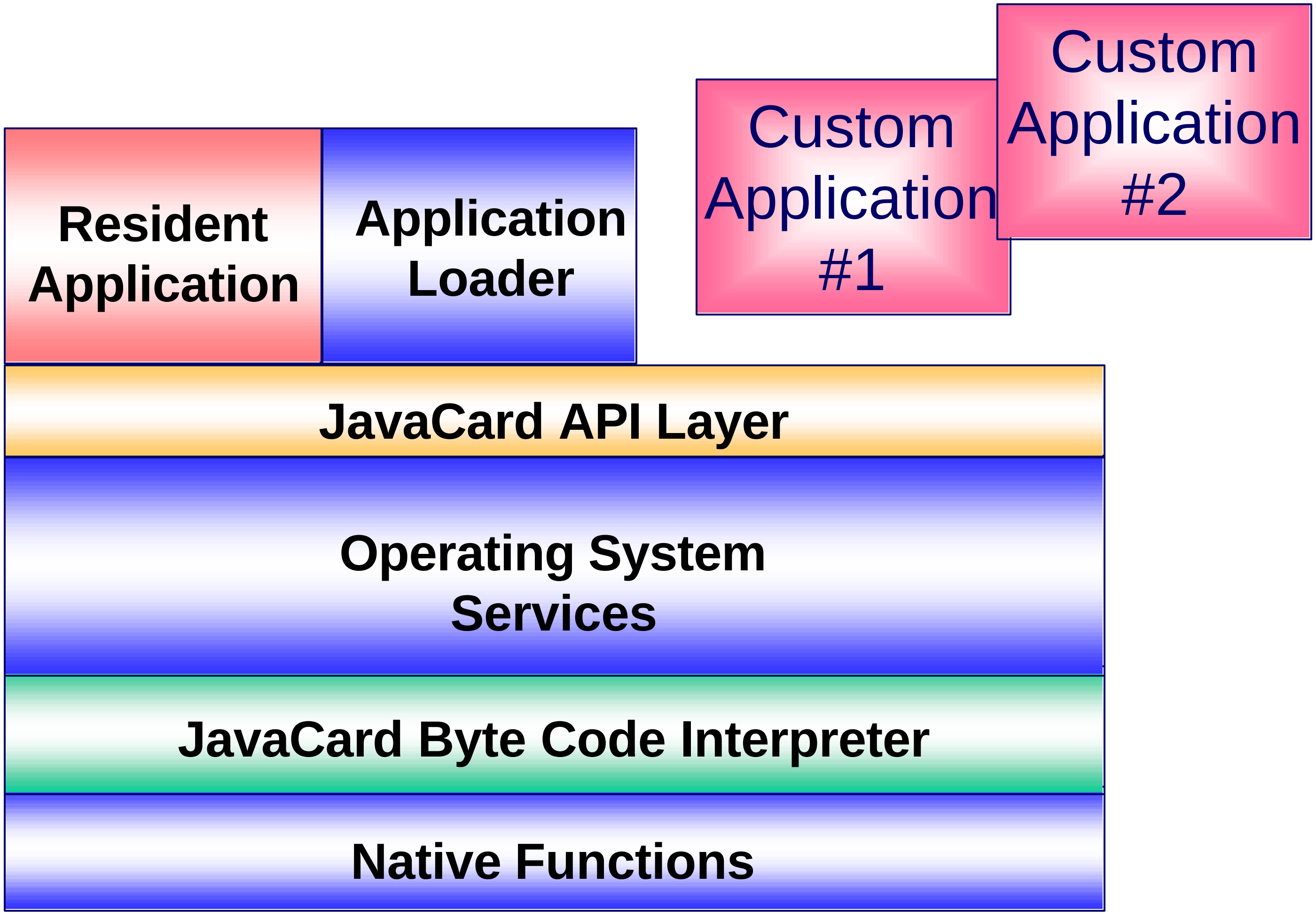
ESN

SRES, ESN, MIN

ESN,MIN -> A

The secret key "A" used to authenticate the subscription never leaves the Smart Card

Open JavaCard Architecture



Resident Application

Application Loader

Custom Application #1

Custom Application #2

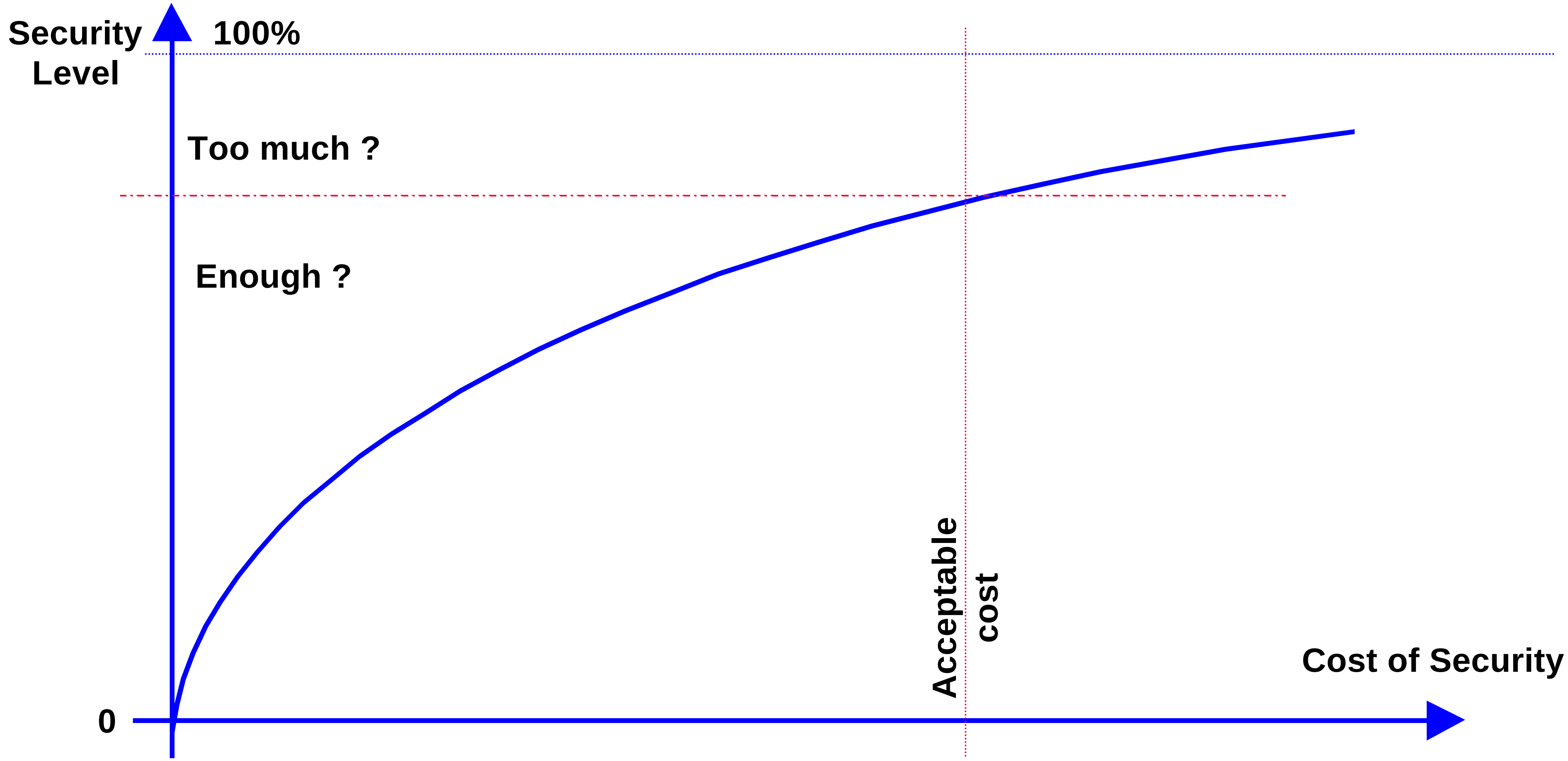
JavaCard API Layer

Operating System Services

JavaCard Byte Code Interpreter

Native Functions

Security Balance



A security system is only as strong as its weakest link